

THE CLAIMS

1. (Previously Presented) A methodology framework for analyzing technology system including a plurality of components and for designing security into that system, the framework comprising:

a first system which identifies the security threats for the solution;

a second system having a security reference model comprising a plurality of interrelated and interdependent security subsystems, the security subsystems further comprising an audit subsystem, an integrity subsystem, and an information flow control subsystem, the second system to determine security properties and functions of the information technology system in terms of the security subsystems;

a third system which is coupled to the second system and which allocates security properties to the components of the information technology system based upon the selected functions which are derived from the nature and number of the security subsystems within the information technology system;

a fourth system which is coupled to the third system for allocating the security properties to the components of the information technology system and which identifies functional requirements for the components, in terms of the Common Criteria, in order to comply with the security properties of the component allocated by the third system; and

a fifth system which is coupled to the fourth system and which documents the requirements for the security components for the information technology system.

1 2. (Previously Presented) A framework for designing security into an information
2 technology system including the elements of Claim 1 wherein the second system which
3 identifies security properties of the information technology system includes a component
4 which uses security subsystems for identifying security properties.

1 3. (Previously Presented) A framework for designing security into an information
2 technology system including the elements of Claim 2 wherein the standard criteria for
3 identifying security properties includes a system which maps functions of security
4 subsystems to an ISO standard 15408, also known as Common Criteria.

1 4. (Previously Presented) A framework for designing security into an information
2 technology system including the elements of Claim 1 wherein the framework further
3 includes a system which documents the solution and the security assumptions using a
4 solution design security methodology.

1 5. (Previously Presented) A framework for designing security into information technology
2 system including the elements of Claim 4 wherein the framework further provides
3 integrity assurance requirements using a standard set of criteria.

1 6. (Previously Presented) A framework for designing security into an information
2 technology system including the elements of Claim 5 wherein the standard set of criteria
3 are in accordance with ISO 15408.

7. (Currently Amended) A computer implemented method of designing security for an information technology system which includes insecure components, the steps of the method comprising:

documenting a solution environment and a plurality of security assumptions using one or more computer-implemented design tools;

identifying, documenting and ranking one or more ~~the~~ security threats to the ~~system~~ solution environment;

determining ~~the~~ one or more security properties of the solution environment within a security reference model comprising a plurality of interconnected and interdependent security subsystems that, inter alia, manage audits, integrity, and information flow control;

assigning functional details of the plurality of interconnected and interdependent security subsystems to an infrastructure, a plurality of components, and a plurality of operations of the ~~system~~ solution environment;

enumerating security requirements for each of the infrastructure, components and operations of the solution environment;

developing integrity assurance requirements for the solution environment; and

~~creating at least one functional technology diagram to document~~ documenting the security requirements and the rationale for the ~~system~~ solution environment;

providing guidance for selection of the plurality of components, for integrating the plurality of interconnected and interdependent security subsystems, and operating the solution environment.

1 8. (Currently Amended) ~~A method of designing a secure solution including the steps of~~
2 ~~Claim 7 wherein the method further includes the step of ranking the security threats to the~~
3 ~~overall system and considering the biggest threats to the security properties of the overall~~
4 ~~system in terms of the security subsystems~~ The method of claim 7 wherein the step of
5 identifying, documenting and ranking one or more security threats to the solution
6 environment further comprises contrasting a normal process flow of a trusted
7 environment with a peril process flow having conditions or exceptions of the normal
8 process flow.

1 9. (Currently Amended) The computer implemented ~~A method of designing a secure~~
2 ~~system including the steps of Claim 8 wherein the step of ranking the security threats to~~
3 ~~the security properties of the overall system includes the step of doing less for security~~
4 ~~threats not considered substantial threats to the security properties of the overall system in~~
5 ~~terms of the security subsystems~~ The computer implemented method of designing
6 security into an information technology system of claim 7 wherein the step of determining
7 one or more security properties of the interconnected and interdependent subsystems that
8 manages audits further comprises designing the capability to initiate an audit, collect
9 audit data, analyze audit data, request a trusted time, archive audit data, and sign and
10 timestamp audit data, generate an audit report, and signal anomaly events of the solution
11 environment.

1 10. (Currently Amended) ~~A method of designing a secure system including the steps of~~
2 ~~Claim 7 wherein the method further includes the step of documenting the system~~

environment and security assumptions and using the environment and security assumptions in developing the security properties of the overall system The computer implemented method of designing security into an information technology system of claim 7 wherein the interconnected and interdependent subsystem that manages integrity further comprises a confirming element to confirm hardware and software components and data integrity, a monitoring element to monitor hardware and software component reliability, a verification element to verify correct operation, a separation element to ensure domain separation, a first clock to maintain trusted time, and a second clock to provide current trusted time.

11. (Currently Amended) ~~A method of designing a secure system including the steps of Claim 7 wherein the method further includes the step of developing integrity assurance requirements for the system and using those integrity assurance requirements in the functional technology diagram(s) for the system.~~ The computer implemented method of designing security into an information technology system of claim 10 wherein the interconnected and interdependent subsystem that manages integrity further has the capability to request a trusted time, receive input of a time-based integrity event, signal an integrity system anomaly, and request an audit of the subsystem that manages integrity.

12. (Currently Amended) ~~★~~ The computer implemented method of securing a solution including the steps of Claim 7 wherein the step of determining the security properties of the overall system includes the step of using standard criteria for evaluating the solution.

13. (Currently Amended) ~~★~~ The computer implemented method of securing a solution including the steps of Claim 12 wherein the step of determining the security properties of the overall system includes the step of using the Common Criteria of ISO Standard 15408.

14. (Currently Amended) ~~★~~ The computer implemented method of securing a system including the steps of Claim 7 wherein the step of enumerating security requirements for infrastructure, components and operations includes the step of using an industry standard security criteria.

15. (Currently Amended) ~~★~~ The computer implemented method of securing a system including the steps of Claim 14 wherein the step of using an industry standard security criteria includes the step of using Common Criteria which conforms to ISO Standard 15408.

16. (Currently Amended) ~~A method of securing a system including the steps of Claim 7 wherein the step of enumerating security requirements for infrastructure, components and operations includes the step of identifying, enumerating and describing a number of security subsystems that in total represent the security function of the solution. The~~ computer implemented method of designing security into an information technology system of claim 7 wherein the interconnected and interdependent subsystem that manages information control further comprises an element that identifies and authenticates an

8 origin/recipient of information control, obtains the identifier/identity of the
9 origin/recipient, and checks the validity of the identifier/identity.

1 17. (New) The computer implemented method of designing security into an information
2 technology system of claim 16 wherein the interconnected and interdependent subsystem
3 that manages information control further comprises an element that checks one or more
4 rules of information flow control rules, and decides to enable or reject the information
5 flow request.

1 18. (New) The computer implemented method of designing security into an information
2 technology system of claim 17 wherein the interconnected and interdependent subsystem
3 that manages information control further enables the information flow request, applies
4 information flow control mechanisms, activate information flow and protection activities,
5 invoke and information flow interface and generate information flow audit data.

1 19. (New) The computer implemented method of designing security into an information
2 technology system of claim 18 wherein the information flow and protection activities are
3 selected from the group comprising: data integrity, privacy, trusted path, trusted channel,
4 proof of origin, proof of receipt, security attributes, immovability, domain crossings,
5 static validation, and content scan/filters.

1 20. (New) The computer implemented method of designing security into an information
2 technology system of claim 7 further comprising using a systems integration system and

3 method that provide in a first phase, the security reference model is used to address a
4 plurality of security requirements of the information technology system; in a second
5 phase, the security reference model is utilized to create a solution environment which
6 specifically addresses security requirements within the solution environment; and in a
7 third phase, a plurality of processes of the interconnected and interdependent security
8 subsystems are measured, monitored and controlled based upon the security reference
9 model.